UEM DEPLOYMENT BEST PRACTICES

Although embarking on a modern work initiative can seem like exploring unchartered territory, the right unified endpoint management (UEM) solution can help you quickly move forward on your journey to becoming a modern, mobile enterprise. Deploying a UEM solution is best achieved by following the four steps outlined here.

PLAN

Are your employees experienced with mobile devices and modern operating systems?

Which modern operating systems, mobile devices, and desktops will your organization support?

How complex is your network infrastructure?

How mature is your IT governance framework, policies, and processes?

DESIGN

Can your IT organization develop and deploy mobile enterprise apps?

How effective are your employee education and training resources?

Does your IT team have experience with certificate authentication?

What are your organization's security requirements?

Define Roles:
- How many admins are required to support this effort?
- What are their individual responsibilities?

Define Visibility:
- Which users and devices will each admin view and report on?

Assign Actions
- What actions each admin can take?

Manage Distribution
- What apps, policies, configurations can each admin distribute to users/devices?

DEPLOY

On-prem deployment?

Cloud-based deployment?

ROLLOUT

Does your help desk staff understand multi-OS management issues?

Can your help desk staff engage with device experts as needed?

Does your help desk staff have access to the resources they need in order to provide the expected level of support?

Does your help desk staff have access to ongoing education opportunities, so that they are able to stay up-to-date on the latest trends?

MobileIron

MobileIron unified endpoint management (UEM) enables your employees to enjoy seamless access to business apps and data through secure mobile devices, desktops, and cloud services while still maintaining complete control over their privacy.

MobileIron UEM Bundles	Silver	Gold	Platinum
On-prem and cloud-based UEM deployment options	✓	✓	✓
Sentry is an inline gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems.	✓	✓	✓
Apps@Work is an enterprise application storefront that manages both in-house developed apps and third-party business apps that can be delivered to users.	✓	✓	✓
AppConnect is a secure business app container with app-specific VPNs for AppConnect-enabled apps.		✓	✓
Email+ is a secure mobile productivity apps package that includes email, contacts, calendar, and tasks for iOS and Android devices.		✓	✓
Docs@Work enables you to access, annotate, share, and view documents across a variety of email, on-prem, and cloud content management systems.		✓	✓
Web@Work is a secure enterprise mobile browser that enables end users to access internal web resources quickly and easily.		✓	✓
Manage macOS desktops across the entire lifecycle: provisioning, configuration, security and control, application deployment, monitoring and compliance, and end-of-life.		✓	✓
Help@Work allows users to share their screens with a help desk agent for more efficient troubleshooting and faster problem resolution.			✓
Tunnel provides per-app VPN capabilities so that you can authorize specific apps to access corporate resources behind the firewall without any end-user intervention.			✓
MobileIron Monitor is a comprehensive, dashboard-based solution that allows you to maintain the health of all your mission-critical MobileIron UEM components.			✓
ServiceConnect Integrations enable you to streamline IT workflows with the MobileIron App for Splunk Enterprise and integrations with ServiceNow.			✓
MobileIron Bridge allows you to leverage existing Group Policy Objects (GPO) scripts to enable granular security and management of Windows 10 PCs.	Add on SKU, requires MobileIron UEM bundles		
MobileIron Access provides secure, conditional access control for cloud services such as Microsoft Office 365, Salesforce, Google Apps for Work, Box, and others.	Add on SKU, requires MobileIron UEM bundles		
MobileIron Threat Defense enables you to protect company data by detecting and remediating known and zero-day threats on mobile devices without internet connectivity required, and no need for users to take any action.	Add on SKU, requires MobileIron UEM bundles		

MobileIron Enables Your Modern, Mobile Enterprise

MobileIron UEM

Harness the power of secure modern devices, apps and cloud services to enable business innovation.
https://www.mobileiron.com/en/solutions/enterprise-mobile-management-emm

MobileIron ACCESS

Secure, conditional access control for cloud services such as Microsoft Office 365, Salesforce, G Suite, Box, and others.
www.mobileiron.com/en/access

MobileIron THREAT DEFENSE

With one app, enterprises can protect company data by detecting and remediating known and zero-day threats on the mobile device, and no need for users to take any action.
https://www.mobileiron.com/en/threat-defense

MobileIron BRIDGE

Leverage existing Group Policy Objects (GPO) scripts to enable granular security and management of Windows 10 PCs.
www.mobileiron.com/en/bridge

MobileIron

401 East Middlefield Road • Mountain View, CA 94043
www.mobileiron.com • globalsales@mobileiron.com

Tel: +1.877.819.3451
Fax :+1.650.919.8006